C-A OPERATIONS PROCEDURES MANUAL

ATTACHMENT

9.6.1.c Fault Tree Analysis

Text Page 2 through 3

C-A-OPM Procedures in which this Attachment is used.		
9.6.1		

Hand Processed Changes

HPC No.	Date	Page Nos.	Initials
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Approved: _____***Signature on File***_____ _____
Collider-Accelerator Department Chairman Date

A. Etkin

FAULT TREE ANALYSIS

Introduction

The purpose of the fault tree analysis is to identify each event and fault which, singly and in all combinations, could cause a specified undesired event. The fault tree analysis is a deductive analytical technique which is qualitative in nature, but can easily be quantified if desired. A fault tree analysis does not model all possible system failures, but only models those faults which can contribute to the specified top event. Hence, proper identification of the top event and events that can individually or in combination with others contribute to the top event.is essential for complete system hazard identification.

Procedure

The fault tree analysis is a deductive analytical technique. The fault tree results in a graphic and logical representation of the various combinations of possible events, both fault and normal, occurring within a system, which can cause a predefined undesired event. An undesired event is any event which is objectionable or unwanted, such as a potential accident, hazardous condition, or undesirable failure mode. The system is reviewed to determine the conditions, events, and failures that could contribute to the occurrence of the undesired event. These contributing conditions, failures and events are then modeled in a logic tree or diagram, showing their relation to each other and the undesired event being analyzed. The process begins with the immediate necessary and sufficient events that could directly cause the undesirable event (first level). As the procedure goes back step-by-step, combinations of events and failures that could cause the top event. Each part of the system and each condition capable of producing an event is examined for its contribution to the top event and for possible improvement to increase the number of contributions (thereby reducing the probability of occurrence) necessary to cause the event. Suitable mathematical expressions representing the fault tree logic events are developed using Boolean algebra. This helps to determine and quantify common mode failures. The resulting mathematical expression of the AND/OR relationships for the tree are then simplified. Probabilities of occurrence are developed for each event in the fault tree and used to compute the probability of occurrence of the top event.

Based upon the information derived from the fault tree evaluation, decisions must be made concerning the adequacy of safety. The design must be approved for safety, and the problem areas must be identified. If the problem areas are identified as unacceptable, corrective action must be taken prior to system operation. Corrective action results in development of preventive measures. Preventative measures are listed below. Engineered features are preferred over administrative controls:

- safety design features
- safety devices
- protective systems
- warning devices
- special procedures

As recommended preventive measures are incorporated into the design, their adequacy in solving the safety problem must be verified. This is done by making the appropriate changes to the fault tree logic diagram and re-evaluating the fault tree.

Documentation

Documentation of the fault tree consists of the following:

- fault tree logic diagrams
- fault tree probability calculations (for quantitative analysis)
- failure/event rate calculations and/or empirical data used to determine probability of occurrence for contributing events
- details of safety improvements
- summary of the final system configuration and the qualitative and quantitative results of the final fault tree analysis.